James P. Flynn, Esquire
EPSTEIN BECKER & GREEN, P.C.
One Gateway Center
Newark, NJ 07102
(973) 642-1900 (phone)
(973) 642-0099 (fax)
Counsel for Novartis Pharmaceuticals Corporation

Russell Beck, Esquire
Stephen D. Riden, Esquire
BECK REED RIDEN LLP
155 Federal Street, Suite 1302
Boston, MA 02110
(617) 500-8660 (phone)
(617) 500-8665 (fax)
Of Counsel for Novartis Pharmaceuticals Corporation (Pro Hac Vice Pending)

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

NOVARTIS PHARMACEUTICALS CORPORATION, Plaintiff, v. ALISHA ALAIMO, Defendant.	)	Civil Action No.: _____

DECLARATION OF FORENSIC EXPERT, ALEXANDER BARNETT

I, Alexander Barnett, affirm as follows:

1. My name is Alexander Barnett. I am over the age of 18. All statements of fact made herein are based on my personal knowledge, or, where indicated, based on my investigation, in which case I believe them to be true.

2. I make this declaration on behalf of Novartis Pharmaceuticals Corporation, a

Delaware corporation with its principal place of business in East Hanover, New Jersey ("Novartis") in support of its emergency motion for order to show cause with temporary restraints.

BACKGROUND

3. I am a forensic consultant for KrolLDiscovery, LLC ("KrolLDiscovery") and work from its offices at 300 Harmon Meadow Blvd, Suite 305 in Secaucus, New Jersey 07094. KrolLDiscovery is an international end-to-end eDiscovery and forensics services and solutions provider.

4. I specialize in computer forensics, *i.e.*, conducting analysis of legal evidence found in computers, digital storage media, and on the Internet. I have been engaged in computer forensics for approximately 6 years. A true and accurate copy of my CV is attached hereto as Exhibit A.

5. I hold a Master's degree in Computer and Information Technology, specializing in Computer Forensics from Purdue University and a Bachelor's degree in Computer and Information Technology, specializing in Network Engineering, from Purdue University.

6. I also hold the following certifications:

- EnCE, which shows proficiency in the usage of EnCase 7 to conduct forensic investigations as well as knowledge of general forensic standards and procedures.
- NeDC, which shows proficiency in the usage of Nuix eDiscovery as well as knowledge of general eDiscovery standards and practices.
- AME, which shows proficiency in the usage of AccessData

Mobile Examiner, a mobile device forensic tool.

- A+, which shows competency in personal computer repair and maintenance.

7. KrolLDiscovery has been retained by counsel for Novartis to examine electronic evidence relating to its former employee, Alisha Alaimo ("Alaimo"). KrolLDiscovery is being paid on an hourly basis for my time. Neither KrolLDiscovery's compensation nor my compensation is contingent in any way upon the outcome of this case.

FORENSIC REVIEW

8. On July 11, 2017, KrolLDiscovery received from Novartis a Lenovo laptop, model number X260, with serial number PC0EPHLE. This laptop contained a Samsung hard drive, model MZ-7TY2560, with serial number S307NWAH816581. I understand that this laptop was the laptop that Alaimo used most recently in connection with her Novartis employment.

9. The laptop was imaged in a forensically sound manner using AccessData FTK Imager 3.4.2.6 ("FTK Imager"). FTK Imager is a third-party imaging tool commonly used in the digital forensics industry. FTK Imager made a bit-for-bit forensic image of the hard drive of the laptop. The original drive was mounted to a Tableau forensic write blocker as "Read-Only," which ensured that the contents of the original drive were not altered. The forensic image was examined using EnCase 7 and Internet Evidence Finder v6.9, software applications used for the forensic analysis of digital evidence.

INTERNET BROWSING HISTORY

10. The laptop imaged was processed with Internet Evidence Finder v6.9. Internet Evidence Finder (IEF) is a third-party tool produced by Magnet Forensics and is widely used throughout the industry to analyze Internet activity artifacts found on computer systems.

11. Evidence shows that Alaimo performed the following Google searches in the months leading up to her departure from Novartis:

Date	Search Term
12/15/16	"biogen"
12/23/2016	"anti compete clause"
12/26/2016	"novartis market cap"
12/26/2016	"ceo biogen"
2/10/2017	"michel biogen"
3/6/2017	"karen lewis biogen"
3/6/2017	"spinraza pricing"
3/8/2017	"biogen address"
3/13/2017	"al biogen"
4/18/2017	"biogen us headquarters"
5/1/2017	"biogen stock"

USB STORAGE DEVICES

12. External USB storage devices, such as USB flash drives, USB thumb drives, and external hard drives, are typically used for transporting and storing data. Common USB storage devices today have different storage capacities ranging from 1 GB to 1 TB or more. USB storage devices are often large enough to back up the entire contents of a computer's hard drive.

13. In my experience, it is common for employees, particularly employees planning to leave a company, to use external USB storage devices and external USB hard drives to transport data.

EVIDENCE OF ATTACHMENT OF USB STORAGE DEVICES TO NOVARTIS LAPTOP

14. The Novartis Laptop was reviewed, therefore, to determine whether USB storage devices had been connected to it and, if so, which devices.

15. Evidence shows that over the lifetime of the custodian's user account (i.e., from November 15, 2016 through June 9, 2017), a total of 7 USB storage devices appear to have been connected. At least four of those were connected between March 12, 2017 (three months after the Google search for "anti compete clause" was conducted) and June 9, 2017 (Alaimo's last day in the Novartis office).

16. Alaimo plugged in one USB device, the Lexar USB Flash Drive USB Device, on June 4, two days *after* she had resigned from her position at Novartis.

17. A chart showing the device plug-ins between March 12, 2017 and June 4, 2017 is below:

Serial #	Device	Last Connected
AAHRXTEZZBKKLB3H&0	Lexar USB Flash Drive USB Device	6/4/2017 13:04
6&1a582251&0	IS817 innostor USB Device	5/19/2017 20:13
0416KK00000055001360&0	PNY USB 2.0 FD USB Device	3/12/2017 18:00
575837314335325636323836&0	WD My Passport 0748 USB Device	(Installed) 4/1/2017 10:04[1]

ACCESSED FILES AND FOLDERS ON THE NOVARTIS LAPTOP

18. I also used EnCase 7 to determine the dates that files on the Novartis Laptop were last accessed in or around the time that the USB devices (including the hard drive) were last inserted between March 12, 2017 and June 4, 2017.

19. My review of these files was limited by the fact that a file or folder's "last accessed" time stamp only reflects the most recent time of access, so it is possible that files

[1] The last connection date of this device was not found, however the USB device installation log shows an installation date of 04/01/17 at 10:04.

accessed on the date a drive was connected may no longer reflect that time stamp due to the file being accessed more recently.

20. The review of the last accessed documents on Alaimo's Novartis Laptop revealed the following:

- Seventeen files and folders were last accessed on 03/12/2017 from 18:00 to 23:59. These file all appear to be system files and folders, with the exception of one video file (1215934362001_2619659992001_The-Westin-Governor-Morris--Morristown-Aug5-2013---1145[1].mp4) and one document (M_Radney Mar 12.docx)
- Thirty-nine files and folders were last accessed on 04/01/2017 from 10:04 to 23:59. These files all appear to be system files and folders.
- Thirteen files and folders were last accessed on 05/19/17 from 20:13 to 23:59. There were two LNK files accessed showing access to a pay statement located on external media (D:\2017-05-12 AAA NVS Pay Stmt.pdf), as well as the root of the external media (D:\).
- Five files and folders were last accessed on 06/04/17 from 13:04 to 23:59. These all appear to be system files or folders.

21. I used EnCase 7 to review other system artifacts that were access on or around the time of known USB storage device insertion dates. These artifacts include LNK files and Shellbag artifacts.

- LNK files are a type of shortcut file that can be automatically created by the system when the user accesses files or folders located on external media or network storage locations.
- Shellbag artifacts are a type of system registry artifact that are created when the user browses a folder with Windows Explorer. These artifacts can contain information such as folder names and time stamps.

22. Although we are still in the process of investigating, we have already determined that the following artifacts are potentially relevant:

- Shellbag artifacts show access to the C:\Users\alaimal1\AppData\Local\Microsoft\Outlook folder on 04/01/17 at 10:17 (thirteen minutes after the WD My Passport drive was first inserted). This folder contains the custodian's Outlook OST file. An OST file is a file container used by Microsoft Outlook to store email. It is my opinion that it is unusual for a user to access this folder and would not access it in the course of normal activities. Given the proximity to the WD My Passport drive installation event, it is reasonable to assume that the OST file could have been copied to the external drive.
- Shellbag artifacts show access to three folders on external media (D:\TrueDelete, D:\data and D:\New folder) at 12:48 and 12:49 on 04/01/17. Over the next eight minutes, the user appears to access many folders on the laptop. Some of these folders then appear to be accessed on the external storage device. Multiple folders with identical names appear to be accessed

over the eight minutes where one folder is on the laptop and one is on the external storage device. It is my belief that the artifacts show copying files and folders from the laptop to the external storage device.

a) It is reasonable to assume that these folders may have been copied to the WD My Passport device inserted earlier.

- Shellbag artifacts show access to the H:\data network folder on 05/19/2017 at 20:07. The user then accesses their Documents and Documents\Relocation US folder at 20:13. The user also accesses the H:\data\Success network folder at 20:13. The Innostor USB storage device was last inserted on 05/19/2017 at 20:13. It is reasonable to assume that files may have been copied from these folders to the Innostor USB storage device.
- Shellbag artifacts only show the folder names and associated time stamps. I am unable to determine the contents of the folder without access to the external storage device.

ADDITIONAL MATERIALS TO REVIEW

23. When a user copies files to/from a computer to/from a USB device, this specific activity is not typically recorded by the operating system. Therefore, it is not possible to know the entire contents of a USB device, and if any company data was copied to it, without examining the device itself. Thus far, there appear to have been seven USB storage devices plugged in to the computer. In order to provide a complete understanding of what data – past or present – is contained on the USB and external hard drive, access to the actual devices (or a forensic image thereof) is required.

24. Although, through a forensic analysis, I have been able to determine some information, I am limited both by the above-stated limitations and by the fact that forensic evidence (including electronic forensic evidence) is, by its very nature, piecemeal and degrades as computers are used. Therefore, I cannot, with the information I have, determine the full scope of Novartis' materials moved and/or copied by Alaimo. A forensic analysis of all computers, electronic media, and accounts in currently possession of Alaimo will provide the best picture of the degree to which Novartis' data was copied and subsequently used.

25. Based on my many years of experience forensically examining computers, the number of functional USB storage drives inserted into the Novartis Laptop, the fact that at least four of the drives were inserted into the Novartis Laptop in just the three months before Alaimo's departure, and the fact that one USB device was inserted two days after Alaimo's resignation, it is my opinion that Alaimo may have copied and/or may currently possess Novartis' documents. However, I will be unable to confirm the misappropriation of Novartis property without examining the electronic devices and platforms to which Alaimo has or had access.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct and that this declaration was executed this 3rd day of August 2017 at Jersey City, New Jersey.

Alexander Barnett

EXHIBIT A

Alex Barnett

Forensic Consultant
300 Harmon Meadow Blvd Suite 305
Secaucus, NJ 07094

201.259.6834
alex.barnett@krolldiscovery.com

Professional Experience

- **Consultant**, KrolLDiscovery, Inc., March 2014 - Present
  - Reponsible for performing forensic acquisitions of client media, including laptops, desktops, tablets, cell phones, removable media, and network data.
  - Responsible for conducting forensic investigations of client media. Topics of investigation include intellectual property theft, human resource violations, inappropriate usage of company assets, and other forms of fraud and misconduct.
  - Responsible for assisting clients in determing the appropriate scope of devices and locations for collection.
  - Responsible for the preparation of reports and other documentation for presentation to clients.
- **Associate**, Deloitte FAS, June 2011 – September 2013
  - Reponsible for performing forensic acquisitions of client media, including laptops, desktops, tablets, cell phones, removable media, and network data.
  - Responsible for conducting forensic investigations of client media. Topics of investigation included intellectual property theft, human resource violations, inappropriate usage of company assets, and other forms of fraud and misconduct.
  - Responsible for evidence tracking and management.
  - Responsible for conducting client exit interviews to determine locations of responsive data for preservation.

Education

- **Purdue University**, West Lafayette, IN, M.S. Computer and Information Technology*, Cyber Forensics,* 2011
- **Purdue University**, West Lafayette, IN, B.S. Computer and Information Technology*, Network Engineering,* 2009

Continuing Education and Certifications

- **EnCE**, EnCase Certified Examiner (2013 – Present)
- **NeDC**, Nuix eDiscovery Certified Specialist (2016 – Present)
- **ACE**, AccessData Certified Examiner (2013 – 2015)
- **AME**, AccessData Mobile Examiner (2015 – Present)
- **A+**, CompTIA A+ Certified Professional (2003 – Present)

Experience with Computer Forensics Examinations & Procedures

- Over 1000 pieces of media imaged
- Have worked on over 100 forensic investigation cases in both private and public sectors

Testimony & Court Experience

» **Provident, LLC vs. Tim Allen, et al.,** Minneapolis, 2015. Provided deposition testimony.

Technical & Professional Presentations & Articles

» **The Forensic Value of the Windows 7 Jump List,** ICDF2C Conference, Dublin, Ireland, October 2011